Cryptography Assignment

Riya Jana

April 2024

1. **Question1:** If a simple Substitution Cipher is used(with an unknown key) and we intercept the cipher text OXAO, then which of the following four-letter words could be the plain text: JHON, SKID, SPAS, LOOT, PLOP or OSLO?
   Answer: Cipher text is OXAO. As it is a simple substitution cipher so one character mapped to only one character always.
   OXAO may map into "SPAS" or "PLOP" or "OSLO". These are the possible plain text.

2. **Question2:** Which class of ciphers does the Vigenere cipher belongs to?
   Answer: The Vigenere cipher belongs to poly-alphabetic substitution cipher.

3. **Question3:** What is the size of the key-space of the Vigenère cipher with a keyword of lenth 13?
   Answer: Length of the keyword is 13. Letter space from where we choose plain text and key is 26(as alphabets are 26 in quantity).
   Key Space will be 26^{13}.

4. **Question4:** What is the multiplicative inverse of 5 in $\mathbb{Z}_{11}$ and Z_{12}?
   Answer: To check in these two set multiplicative inverse holds or not, we need to check gcd(5,11) and gcd(5,12) is equal to 1 or not. If so then multiplicative inverse holds.
   Now, gcd(5,11)=1
   gcd(5,12)=1
   Multiplicative inverse would be:
   (5x?) mod 11 = 1
   (5x?) mod 12 = 1
   In both of the cases we need to find the "?" value.
   (5x9)≡45(mod 11)≡1 then ans is 9
   (5x5)≡25(mod 12)≡1 then ans is 5

5. **Question5:** State the mathematical form of the Affine Cipher.
Answer: Let, E be encryption function.
D be decryption function.
x be plain text.
y be cipher text.
a be the multiplier.
b be the constant value.
Now, the mathematical formula for encryption and decryption in Affine cipher:
E(x)=y is defined as y=(a.x+b) mod 26
D(y)=x is defined as x=a^{-1}(y-b) mod 26
Condition for affine cipher there should exists inverse of a otherwise its not possible to encrypt.

6. **Question6: (a) Encrypt first 4 letters of your name with the Hill cipher using the following key in Z_{26} :**

$$K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$$

Answer: Plain text = RIYA
Converting it into numeric value: 17 8 24 0 with the key

$$K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$$

As key is 2x2 so at a time we can encrypt two letters. Dividing the plain text into two part:

$$\begin{bmatrix} 17 & 8 \end{bmatrix} * \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} mod 26$$

$$\begin{bmatrix} (17 * 11) + (8 * 3) \\ (17 * 8) + (8 * 7) \end{bmatrix} = \begin{bmatrix} 211 \\ 192 \end{bmatrix} mod 26$$

results to

$$\begin{bmatrix} 3 \\ 10 \end{bmatrix} = \begin{bmatrix} D \\ K \end{bmatrix}$$

In next two letters,

$$\begin{bmatrix} 24 & 0 \end{bmatrix} * \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} mod 26$$

$$\begin{bmatrix} (24 * 11) + (0 * 3) \\ (24 * 8) + (0 * 7) \end{bmatrix} = \begin{bmatrix} 264 \\ 192 \end{bmatrix} mod 26$$

results to

$$\begin{bmatrix} 4 \\ 10 \end{bmatrix} = \begin{bmatrix} E \\ K \end{bmatrix}$$

Finally the cipher text will be DKEK.

(b) Now, show the steps to calculate K^{-1}

Answer: Here k^{-1} is inverse of the square matrix K formula for k^{-1} is:

$$K^{-1} = \frac{1}{\text{Det}(K)} * \text{Adj}(K)$$

step1: Finding determinant of K:
(11x7 - 8x3) mod 26 = 1
step2: Finding Adj of K:

$$\begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} mod26 = \begin{bmatrix} 7 & -8 \\ -3 & 11 \end{bmatrix} mod26 = \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix}$$

step3: Finding inverse of K:

$$K^{-1} = \frac{1}{\text{Det}(K)} * \text{Adj}(K)$$

$$K^{-1} = \frac{1}{1} * \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} = \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix}$$

(c) What are the necessary condition for K to be invertible.

Answer: If the Det of K is non-zero then only we can say that K is invertible.

7. **Question7: (a)Suppose π is the following permutation of {1...8}**

x	1	2	3	4	5	6	7	8
$\pi^(x)$	4	1	6	2	7	3	8	5

Compute the permutation π^{-1}:

Answer:

x	1	2	3	4	5	6	7	8
$\pi^{-1}(x)$	2	4	6	1	8	3	5	7

(b) Decrypt the following ciphertext, for a Permutation Cipher with m = 8, which was encrypted using the key π:
TGEEMNELNNTDROEOAAHDOETCSHAEIRLM

x	1	2	3	4	5	6	7	8
Cipher text	T	G	E	E	M	N	E	L
Plain text	E	T	N	G	E	E	L	M

x	1	2	3	4	5	6	7	8
Cipher text	N	N	T	D	R	O	E	O
Plain text	D	N	O	N	E	T	O	R

Answer: Breaking 32 letter cipher text into 8 letter blocks.
step1: step2

step3

step4 Finally our plaintext is ETNGEELMDNONETORDAEATHCOESRHLAMI.

x	1	2	3	4	5	6	7	8
Cipher text	A	A	H	D	O	E	T	C
Plain text	D	A	E	A	T	H	C	O

x	1	2	3	4	5	6	7	8
Cipher text	S	H	A	E	I	R	L	M
Plain text	E	S	R	H	L	A	M	I